



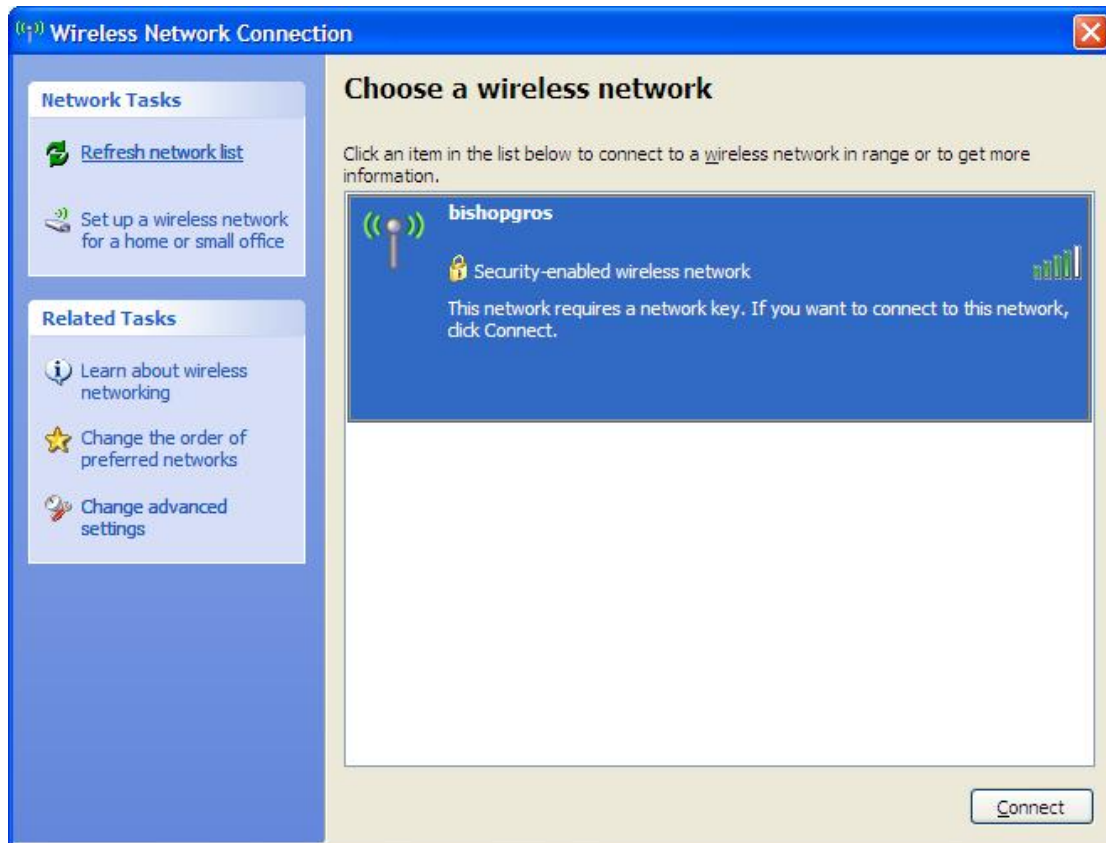
BISHOP  
GROSSETESTE  
UNIVERSITY



## BG Wi-Fi Service User Guide

The University has been equipped with a number of Wireless Access Points. The closer you get to an access point the stronger the signal you will receive on your laptop or computer.

1. You can search for the BG Wi-Fi by using the Windows Wireless Utility, look for the SSID '**bishopgros**' as below:

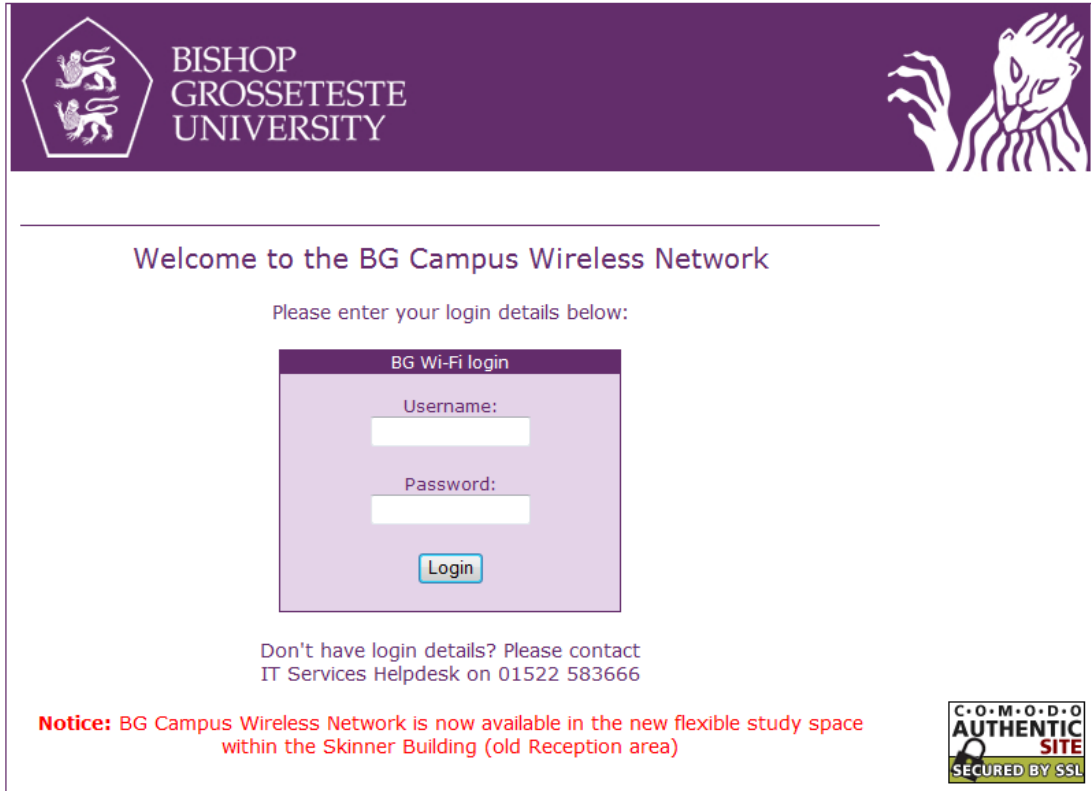


2. Select '**bishopgros**' and click on Connect, you will be prompted to provide the WPA encryption key code.
3. WPA Code is **Spr1ngB0k** (where 1 and 0 are Numbers)



4. You will need to enter the code twice, as you type the characters will not be displayed, click 'Connect' again. This Depends on Windows Version you have.

5. You should then be connected to the BG Wi-Fi network. **All the settings above will only need to be completed once; your system will remember these details for future use.**
6. Open a web browser and you should automatically be redirected to a secure login page where you will need to agree to sign a security certificate, and then enter your username and password within the login dialogue box on the centre of the page (see screenshot below).



**BISHOP GROSSETESTE UNIVERSITY**

Welcome to the BG Campus Wireless Network

Please enter your login details below:

**BG Wi-Fi login**

Username:

Password:

Login

Don't have login details? Please contact  
IT Services Helpdesk on 01522 583666

**Notice:** BG Campus Wireless Network is now available in the new flexible study space  
within the Skinner Building (old Reception area)

C.O.M.O.D.O.  
**AUTHENTIC SITE**  
SECURED BY SSL

### How do you know that you have signed in successfully?

Having successfully logged onto the BGC Wi-Fi you will notice a small 'Bluesocket' login box has appeared on your screen showing your login name, a pulsing wireless icon, and a 'click to log out' link which is used to terminate your wireless session.



If this does not appear you need to ensure that you have allowed popup from the following addresses:

<https://bluesocket2.bishopg.ac.uk>

If you lose, close or overwrite this window, or if your operating system or browser does not permit the creation of this window, you can logout by entering the following URL into your internet browser:

**<https://bluesocket2.bishopg.ac.uk/login.pl?action=logoutPopup>**

This will take you to the Logout option. You may find it useful to save this link as a personal shortcut or a favourite in your Web browser.

## **Wireless Troubleshooting**

If you open Internet Explorer, and the BlueSocket login page doesn't come up:

### Delete Temporary Internet files:

1. Close the Internet browser.
2. Go to Start > Control Panel > Internet Options > Delete Temporary Internet Files (check "Delete offline content").

### Check to make sure the wireless card is enabled:

1. On newer laptops, with the wireless card onboard (inside), there are usually hotkeys or hardware buttons to press to turn on the wireless antenna. A typical hotkey combination is FN + F2 (look for the key with a wave representation). Hold down the FN key and press the F? key. A wireless indicator light should display somewhere.
2. On machines where the wireless card is attached externally, go to Start > Programs > and look for the Wireless (or wlan) program. Click on the program, and then enable the wireless card (click on "Wireless Enable, or Wireless Off").

### If the wireless antenna does not automatically acquire Bishopgros:

1. From step b) above, or if Windows controls the wireless connection, go to Start > Control Panel > Network Connections > double-click the Wireless Connection.
2. Look for a tab pertaining to available networks (site).
3. Select Bishopgros from available networks and click connect.
  1. In a few seconds, the status of the Bishopgros network should change to "connected".
4. Open up Internet Explorer.
  1. Accept the "Security Alert".
  2. A BlueSocket login page should display. Enter an e-mail address in the upper left-hand corner and click login.

### If the "Available Networks" does not display the Bishopgros network:

1. Click on the Start button > Right-click on My Computer > Properties > Hardware > Device Manager.
2. Expand Network Adapters. Double-click on the wireless adapter.
3. Check to make sure it is enabled and working properly.

If the adapter is working properly:

- The wireless antenna sees the Bishopgros network, but does not connect.
- Click on the Start button > Control Panel > Network Connections.
- Double-click on the Wireless Connection > Properties.
- Select "Internet Protocol (TCP/IP)" > click Properties.
- **Write down these settings in case you need to reconfigure them later.**
- Select the buttons:
  1. Obtain an IP address automatically
  2. Obtain DNS server address automatically
- Click OK, OK, and Close out of the menus until you are back to Network Connections.

Go back to the Wireless program from the Programs menu and attempt a connection to Bishopgros again.

**What if you are still having problems:**

1. You have do not have a firewall or Internet Security package installed which maybe blocking URL redirection.
2. Your security settings on Internet Explorer are not set to high.
3. You do not have any third party Internet Explorer toolbars, such as Google Search, Yahoo and AOL toolbars, these can all cause problems.

# Wireless Network: Notes of Guidance

To be read in conjunction with the IT Systems Acceptable Use Policy and the IT Systems Security Policy

## 1 Introduction

- 1.1 Bishop Grosseteste University College Lincoln provides a wireless computer network for its staff and students. Most areas of the campus are covered: hotspots are indicated by appropriate signs. More detailed information about coverage is available on the University College website.
- 1.2 The IT Services department is responsible for managing all aspects of the wireless network.
- 1.3 These guidelines should be read in conjunction with the **IT Systems Acceptable Use Policy** which is available to view on the University College website.

## 2 How to access the wireless network

- 2.1 All students and staff members wishing to use the wireless network will need to apply by email to IT Services for the necessary encryption key. The key will then be e-mailed to each user together with a copy of these guidelines and instructions on how to connect to the wireless network.
  - 2.1.1 *Resident students*

The halls of residence use a separate wireless network to the rest of the campus, however resident students can connect to both networks using the same procedure. IT Services will provide free anti-virus software and/or personal firewall software to resident students for the duration of their stay in University College residences.
  - 2.1.2 *Non-resident students and staff*

The University College cannot provide wireless cards, and/or anti-virus and/or firewall software to non-resident students or staff wishing to use their own personal computers/laptops to access the wireless network. In these instances users will be expected to provide their own wireless-ready hardware.

## 3 Technical requirements

- 3.1 Computers/laptops must have the following **minimum** specifications to access the wireless network:
  - XP / 7 or Mac OS9 operating system
  - 1000 MHZ CPU
  - 256mb RAM
  - 200mb hard drive space available for drivers
  - DVD/CD-ROM drive
  - USB port 1.1 or 2.0
  - Internet Explorer 8.0 or above
  - A fully patched operating system running the latest service packs

- 3.2 Users of the wireless network must ensure that their computers/laptops are running up-to-date anti-virus software and personal firewall software for the full duration of their access to the wireless network (i.e. for their duration of study or employment).

#### **4 Network performance**

- 4.1 The performance of the wireless network is heavily dependant upon the number of people using it at any one time; if a great many people use a particular access point at the same time processing speeds may be adversely affected.

#### **5 Acceptable use of the wireless network**

- 5.1 Users are responsible for all activity on their wireless network account and should not share or disclose their login details with or to others.
- 5.2 It is expressly forbidden to connect any wireless network device or equipment directly into the wireless network without prior permission from IT Services. Any unauthorised devices will be considered rogue devices and may be subject to removal from the network.
- 5.3 Misuse of the wireless network will be taken extremely seriously and may lead to immediate permanent disconnection of any unapproved wireless networking equipment and/or for any deliberate or repeated breach of policy, disciplinary action under current college regulations. The following text is taken from the IT Systems Acceptable Use Policy:

The following examples of misuse apply specifically to the University College's wireless network:

- configuring wireless cards in 'ad hoc' mode (which allows one user to access another user's mobile device e.g. for gaming purposes);
- running peer-to-peer (P2P) file sharing software, e.g. Kazaa;
- intercepting or attempting to intercept other wireless transmissions for the purposes of eavesdropping;
- accessing or running utilities or services which might negatively impact on the overall performance of the network or deny access to the network, e.g. radio frequency jamming, denial of service;
- provide services which may interfere with normal network operation.

#### **6 Monitoring and security**

- 6.1 In order to limit the potential security risks that may be associated with wireless network technologies, access to the wireless network must take place in a controlled and secure manner. To this end use of the wireless network is monitored by IT Services.
- 6.2 In order to manage and monitor the wireless network, and to identify rogue devices and possible misuse of the network, IT Services will make periodic sweeps of the wireless network coverage areas.
- 6.3 Users of the wireless network are reminded not to leave valuable equipment, including laptops and other wireless devices, unattended on University College premises.

#### **7 Advice and guidance**

- 7.1 All enquiries about the wireless network should be directed to IT Services at [helpdesk@bishopg.ac.uk](mailto:helpdesk@bishopg.ac.uk)
- 7.2 Technical support will be provided by the IT Services department during normal office hours by phone (01522 583666), e-mail ([helpdesk@bishopg.ac.uk](mailto:helpdesk@bishopg.ac.uk)) or in person at the IT Helpdesk.